TRANSMISSION VERIFICATION REPORT

TIME : 08/19/2008 10:23
NAME : PVF
FAX : +1-530-759-1665
TEL : +1-530-759-1660

DATE,TIME	08/19 10:22
FAX NO./NAME	15712702090
DURATION	00:01:20
PAGE(S)	03
RESULT	OK
MODE	FINE ECM

Application Number	: 10/800,315	Confirmation Number: 1742
Applicant	: Daniel ManHung Wong	
Filed	: 10 March 2004	
T.C./A.U.	: 2166	
Examiner	: Raab, Christopher J.	
Docket Number	: OR03-15501	
Customer No.	: 51067	

Proposed Amendment and Interview Summary
Via Fax (571) 270-2090 and Electronic Filing

PROPOSED AMENDMENT AND INTERVIEW SUMMARY

Dear Examiner Raab:

In light of the interview on **22 August 2008**, please find the proposed amendment and an interview summary below.

Identification of Claims and Reference Discussed

Claim(s) for discussion: Claim 1

Reference(s) for discussion: Chaudhuri and Lee.

Applicant's Arguments

Applicant wishes to point out the following distinctions between embodiments of the present invention and Chaudhuri as well as Lee:

First of all, the query signature in the present invention comprises textual

Application Number	: 10/800,315	Confirmation Number: 1742
Applicant	: Daniel ManHung Wong	
Filed	: 10 March 2004	
T.C./A.U.	: 2166	
Examiner	: Raab, Christopher J.	
Docket Number	: OR03-15501	
Customer No.	: 51067	

Proposed Amendment and Interview Summary
Via Fax (571) 270-2090 and Electronic Filing

PROPOSED AMENDMENT AND INTERVIEW SUMMARY

Dear Examiner Raab:

In light of the interview on **22 August 2008,** please find the proposed amendment and an interview summary below.

Identification of Claims and Reference Discussed

Claim(s) for discussion: Claim 1

Reference(s) for discussion: Chaudhuri and Lee.

Applicant's Arguments

Applicant wishes to point out the following distinctions between embodiments of the present invention and Chaudhuri as well as Lee:

First of all, the query signature in the present invention comprises textual SQL keywords and operands without literals (see paragraphs [0038-0039] of the instant application) and is **extracted** from the query itself. In contrast, the signature in Chaudhuri is an integer **derived from and then assigned to** a query (see Chaudhuri col. 7, line 61 – col. 8, line 2; and col. 4, line 62-col. 5, line 5). Moreover, Chaudhury teaches matching two queries by a brute-force text-based string comparison, which does not differentiate SQL keywords from literals in a query (see Chaudhuri col. 7, lines 54-60). The present invention, on the contrary,

generates a signature based on the SQL keywords with literals removed. Furthermore, the Chaudhury system groups queries with the same signatures for performance comparisons (see Chaudhuri col. 5, lines 3-5). The present invention, on the other hand, uses query signatures to determine invalid queries of SQL injection (see paragraphs [0038]-[0040] of the instant application).

Furthermore, Applicant wishes to point out that the fingerprint generation method disclosed by Lee is fundamentally different from embodiments of the present invention. The SQL injection detection system in the present invention produces a signature for a database query by retaining the textual SQL keywords contained in the query, **and removing the field names and values** in the query. Therefore, the signature in the present invention specifies a structure based on operations within the query and is **independent** of the field names and values in the query. However, the fingerprint disclosed by Lee is generated by selectively replacing **only field values, but not field names**, in a query with tokens, hence is **not independent** of the field names in the SQL query (see Lee Section 2.2, page 267-268, especially, the presence of field names "custid" and "amt" in the fingerprint).

Proposed Amendment:

1. (Currently Amended) A method for using query signatures to detect structured query language (SQL) injection, comprising:

initializing a signature cache, wherein initializing the signature cache involves:

trapping database queries in a controlled environment,

parsing the database queries to produce a set of valid signatures, wherein parsing the database queries involves retaining SQL keywords contained in each query, and removing field names and corresponding

values in each query, to determine the signature for each query;

wherein the signature for a query contains the text of SQL keywords and operands without any field name or value in the query. ~~determining signatures for the queries, wherein the signature SQL keywords contained in the corresponding query with literals removed,~~ and

storing the valid signatures in the signature cache;

receiving a query at the database;

parsing the query at the database to determine a signature for the query, wherein the signature comprises SQL keywords contained in the corresponding query with literals removed;

determining if the signature is located in the signature cache, which contains signatures for valid queries; and

if so, allowing the corresponding SQL query to proceed. ~~processing the query.~~ otherwise, triggering a mismatch alert.~~identifying the query as being SQL injected and rejecting the query.~~

Outcome of Interview

<N/A>

Respectfully submitted,

By /Shun Yao /
Shun Yao
Registration No. 59,242
Date: 19 August 2008

Shun Yao
Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
Fax: (530) 759-1665
Email: shun@parklegal.com